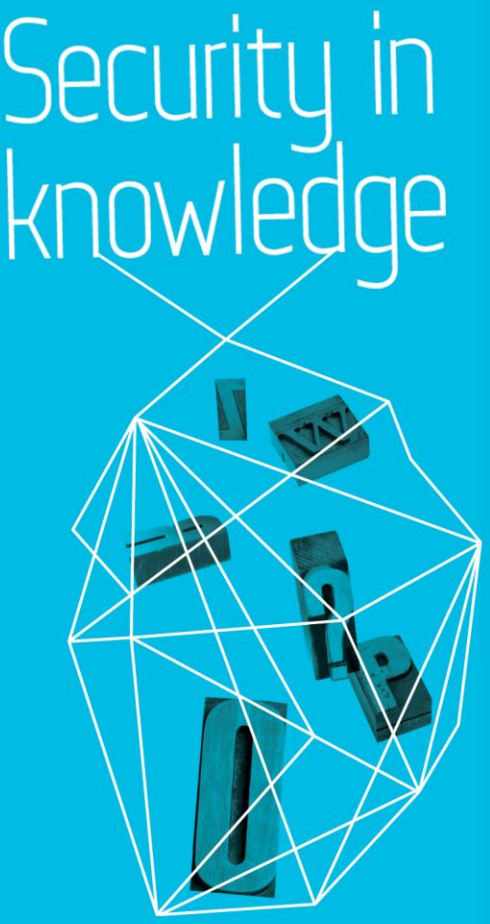
RSA CONFERENCE 2013

The Lessons Learned from Cyber War Malware



Nima Bagheri
Chief Executive Officer, U0vd Security

Session ID: HTA-F41

Session Classification: Advanced

Agenda

- Session Topics:
  - The Big Bang: Stuxnet
  - Information Gathering: Duqu
  - The Paranormal : Stuxnet 3.0
  - The Big Teacher: Flame
  - The Most Complex Worm Ever

The Big Bang: Stuxnet

- The most pernicious computer virus ever known wasn't out to steal your money, credit card information or your passwords. Its target appears to have been the centrifuges in an Iranian nuclear facility. Stuxnet showed, for the first time, that a cyber attack could cause significant physical damage to a facility.

- That’s reason we called that the Big Bang → Stuxnet was not identified by Anti Virus software.

The Idea Behind Stuxnet?

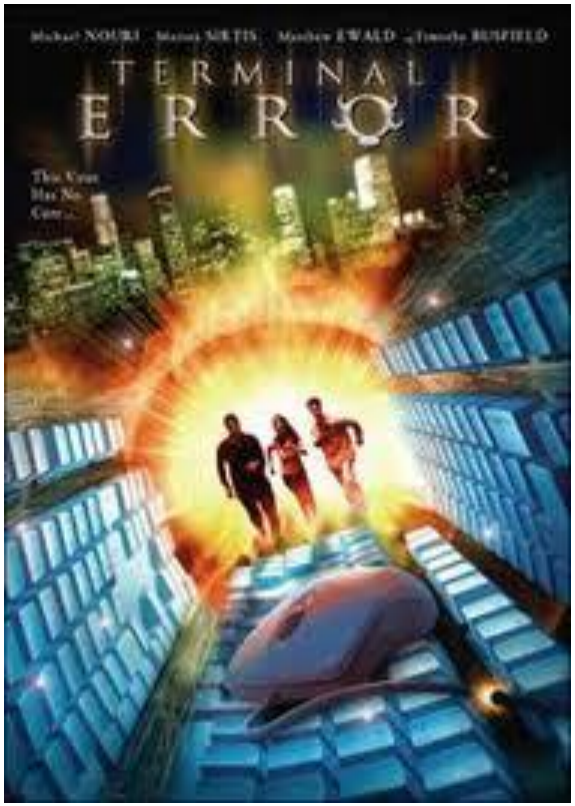
Movie “Terminal Error (2002)”

Wikipedia summary:

> An ex-employee of a computer firm wants revenge and befriends the boss Brad's son Dylan giving him an MP3 file containing a computer virus. This virus creates havoc all across the city by poisoning the water with chlorine, making planes crash and ultimately developing an intelligence of its own.

T.L. Petrie, Screenwriter

> Claimed MP3 infection method was non Executable worm → very similar to Stuxnet.



Identified!

عاملان انتشار ویروس استاکس‌نت شناسایی شدند

پنجشنبه، ۲۹ مهرماه ۱۳۸۹

ایتنا- وزیر ارتباطات و فناوری اطلاعات: افرادی خواسته یا ناخواسته این ویروس را به داخل کشور منتقل کرده‌اند.

Reza Taqhipour
Minister of Communications and Information Technology, Iran

"We identified persons, who transferred Stuxnet to IRAN."

وزیر ارتباطات و فناوری اطلاعات از شناسایی عاملان انتشار ویروس جاسوس، موسوم به استاکس‌نت خبر داد.
رضا تقی‌پور پس از جلسه دیروز هیئت دولت در مصاحبه با واحد مرکزی خبر درباره عامل انتشار این ویروس گفت: مسیر انتشار ویروس استاکس‌نت که از طریق حافظه‌های قابل حمل و فلش مموری بود، شناسایی شده است.
وی افزود: افرادی خواسته یا ناخواسته این ویروس را به داخل کشور منتقل کرده‌اند.

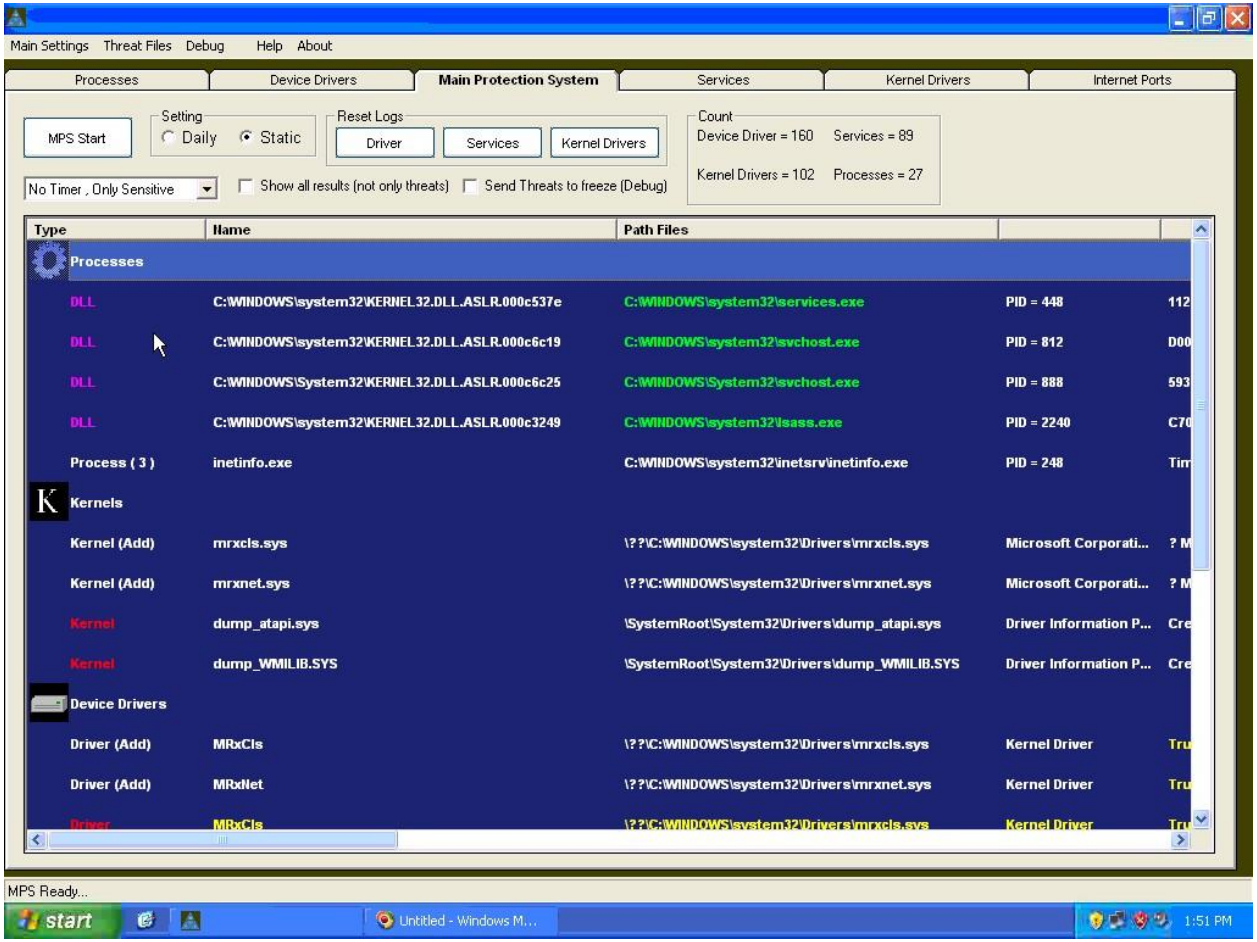
تقی‌پور در خصوص شناسایی این افراد گفت: جریان‌ها شناسایی شده‌اند و اینکه آیا عامدانه بوده یا به صورت سهوی و بدون اطلاع نیز حدودا شناسایی شده است.
وزیر ارتباطات با بیان اینکه این موضوع در مسیرهای لازم در دست پیگیری است، افزود: بدین ترتیب خواهیم توانست از تکرار این موارد در آینده جلوگیری کنیم.

تقی‌پور در پاسخ به سوالی درباره جریان‌های انتشار دهنده ویروس استاکس‌نت گفت: بعضی‌هایشان کارشناسان خارجی بوده‌اند که در مراکز صنعتی تردد داشته‌اند و بعضی هم افراد ناآگاه بوده‌اند که به صورت سهوی و از طریق حافظه‌های قابل حمل این ویروس را منتقل کرده‌اند.

My Relationship to Stuxnet

- First person who released Advisory for Iranian CERT.
- My tool (written in 2009 – not the first) was capable of detecting Stuxnet before the worm had been identified.

Venak Detected Stuxnet Driver



Demonstration

My Conference in Tehran

- My Conference in Tehran: The Black Market of Stuxnet
  - This information is based on Conference research in Tehran

Where we Identified the Stuxnet Infection

Oil & Gas = 2

Power Plants = 1

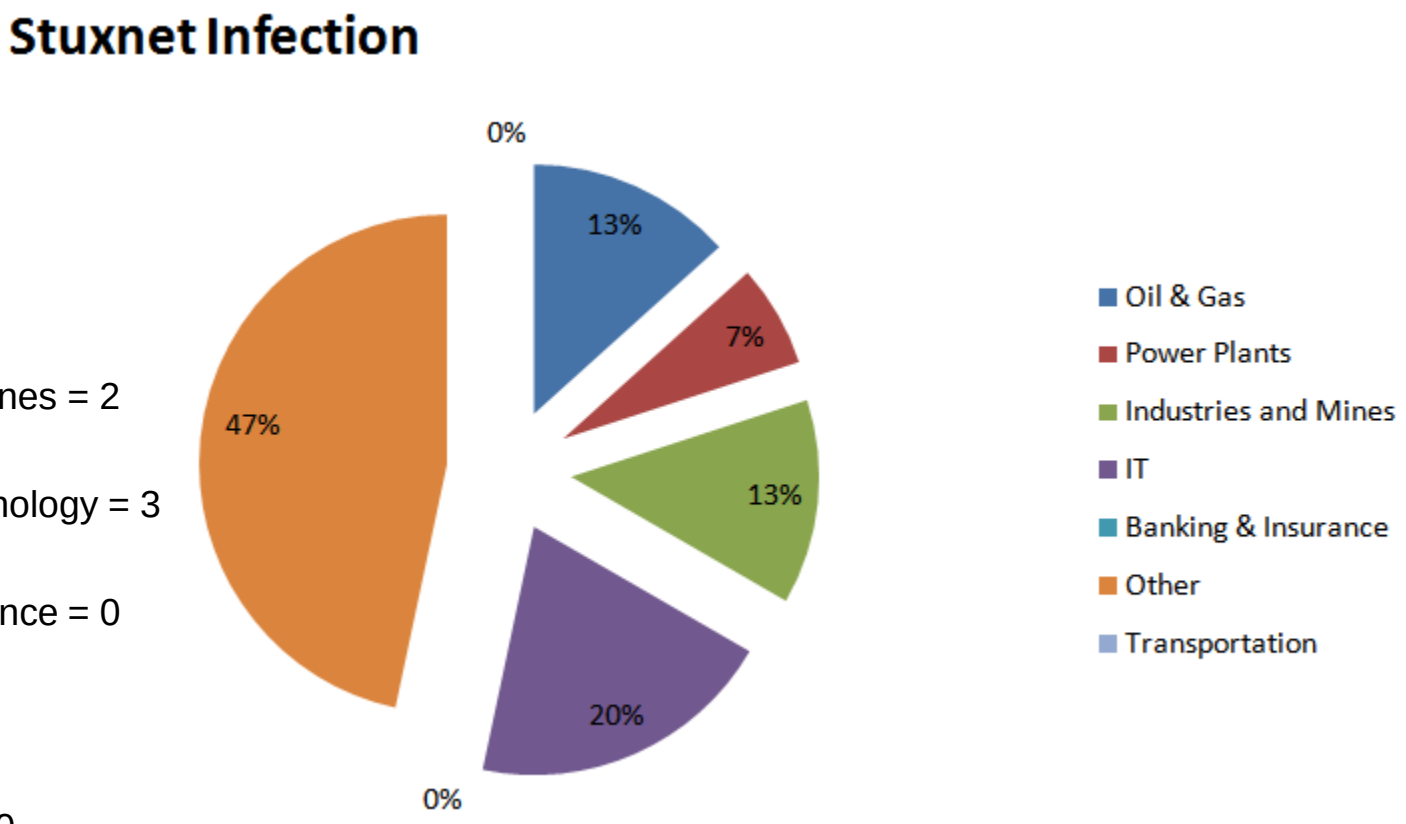
Industries and Mines = 2

Information Technology = 3

Banking & Insurance = 0

Other = 7

Transportation = 0



The Lesson Learned from Stuxnet

- Most AV solutions cannot detect Stuxnet – most current malware works differently
- Most tools ignore signed Kernel and Device drivers,
  - The tools ignore Drivers when target driver had been signed
- Solution → create an alarm for new installed Drivers even if they were signed.

The Game Changer: Duqu

```
class2_ctor     proc near               ; CODE XREF: ...

arg_0_p_compare_func= dword ptr  4

                push    esi
                push    450h            ; dwBytes
                call    new
                mov     esi, eax
                pop     ecx
                test    esi, esi
                jz      short loc_100125B3
                lea     eax, [esi+class_2.csec]
                push    eax             ; lpCriticalSection
                call    ds:InitializeCriticalSection
                mov     eax, [esp+4+arg_0_p_compare_func]
                mov     [esi+class_2.setup_class13], offset class2_setup_class13
                mov     [esi+class_2.append], offset append_to_existing
                mov     [esi+class_2.remove], offset class2_remove ; (this, key)
                mov     [esi+class_2.clear], offset class2_clear
                mov     [esi+class_2.exists], offset class2_exists
                mov     [esi+class_2.count], offset class2_count
                mov     [esi+class_2.get_next_value], offset class2_get_next_value
                mov     [esi+class_2.get_prev_value], offset class2_get_prev_value
                mov     [esi+class_2.get_values_as_array], offset class2_get_values_in_array
                mov     [esi+class_2.dtor], offset class2_dtor
                mov     [esi+class_2.p_compare_func], eax
                call    class2_allocate_block_pair ; 1 = success
                                        ; 0 = fail
                test    eax, eax
                jnz     short loc_100125B7
                push    esi             ; lpMem
                call    class2_dtor
                pop     ecx

loc_100125B3:                           ; CODE XREF: ...
                xor     eax, eax
                pop     esi
                retn
; ---------------------------------------------------------------------------

loc_100125B7:                           ; CODE XREF: ...
                mov     eax, esi
                pop     esi
                retn
class2_ctor     endp
```

Duqu had different Characteristics

- Goal of Duqu seems to be password stealing data-capture malware
- Duqu had different characteristics:
  - Unknown programming language
  - Not compiled with Microsoft's Visual C++ 2008
  - Duqu shows certain characteristics in its coding, injection and behavior that is indicative of the Stuxnet code
  - Stuxnet injects code into PLC Systems to get a kinetic response. There's no evidence of that in Duqu. This looks more like it's data gathering and spying on industrial controller networks.

Duqu had different Characteristics

- Rogue Certificate

  There's not a lot of evidence that it was a stolen rogue certificate. It looks like it was a rogue-created certificate. It means people had access to another certificate authority (CA).

- Different rootkit functionality

  Usermode rootkit functionality, not kernel rootkit functionality. There's a difference in technique, and a difference in how you detect it. With a kernel-mode step, you're going to attack memory spaces and attack kernel table steps and inject your code into the kernel, that's only one way of rootkitting a machine.

The Lesson Learned:

- Encrypt your files!!
- Duqu could not read encrypted files.

The Paranormal : Stuxnet 3.0

- Carl Sagan, Pale Blue Dot: A Vision of the Human Future in Space

The Paranormal : Stuxnet 3.0

- Deep information manipulation
- Transferring information via Command & Control mainly through via search engine optimization and SEO search engines like Bing, Google or Yahoo.
- Free file format exploit with special attention to those file formats that are free and not owned by organizations like AVI format.

Demonstration

Examples:

- 1. Deep information manipulation happened on Gauss Malware

Resource	File name	Description
100	System32.dat (.CatRoot.tmp)	32-bit payload
101	System32.bin (.CatRoot.tmp)	64-bit payload

USB Payload

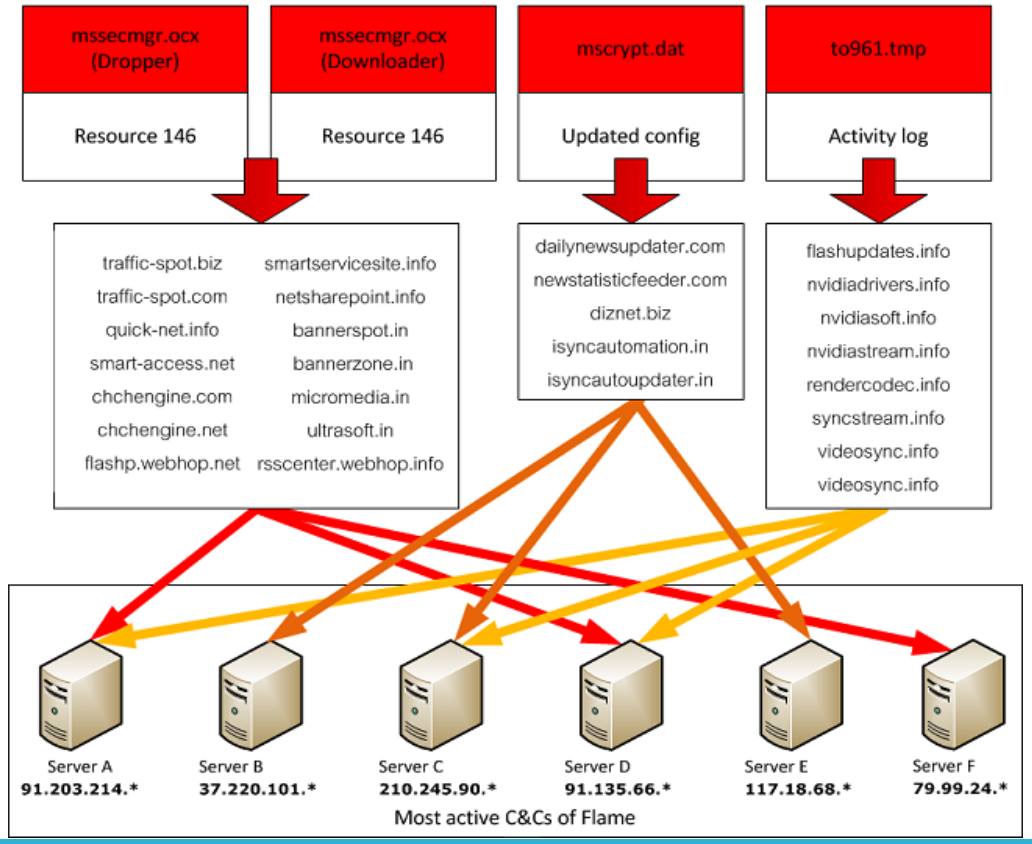
Both 32-bit and 64-bit DLLs implement the same functionality. When loaded using the LNK vulnerability, they start a main thread and return. The main thread copies the payload to %TEMP% directory and loads itself again. When loaded from %TEMP%, it creates a mutex "Isvp4003ltrEvent", patches the "NtQueryDirectoryFile" function in ntdll.dll so that it hides its files and then sends the "F5" key event to windows of classes "SysListView32", "SysTreeView32", "DirectUIHWND", causing Explorer directory listings to refresh. This hides the files. It also waits for the event "Global\RasSrvReady".

Then, it retrieves the following data from the system:

- Version of the Windows OS
- Workstation info
- Network adapter information
- Routing table
- Process list

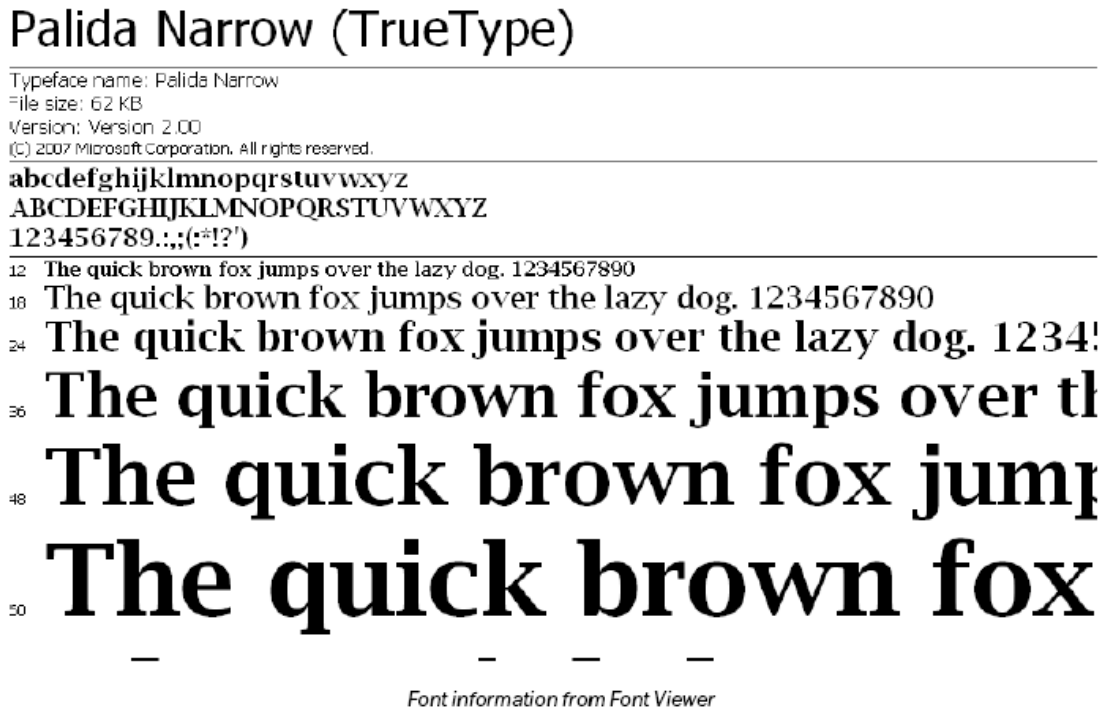
Examples:

- 2.Transferring information via C & C happened on Flamers



Examples:

- 3. Free file format exploit happened in Gauss & Duqu Malwares (Gauss used TTF format and Duqu used Doc)

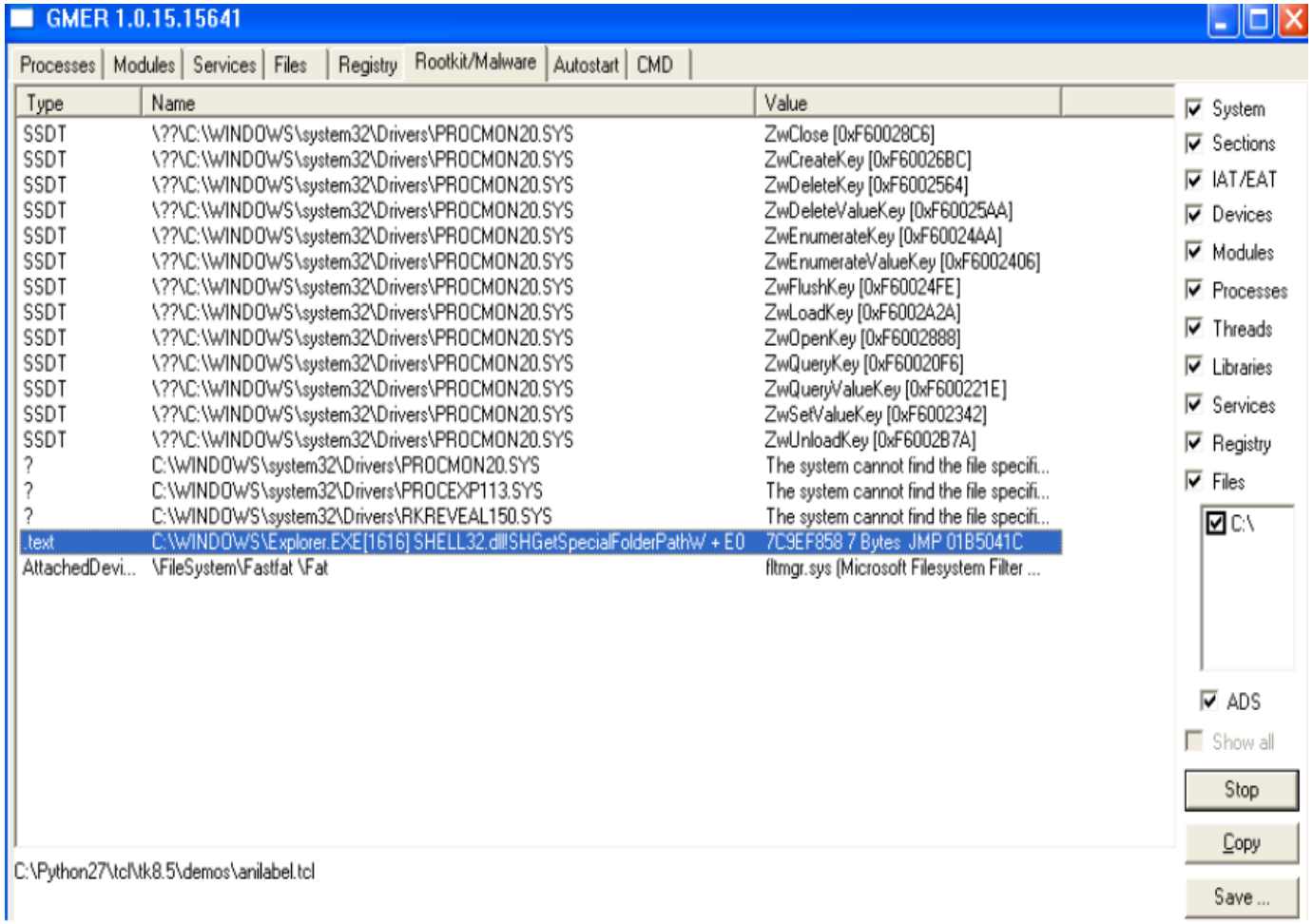

Palida Narrow (TrueType)
Typeface name: Palida Narrow
File size: 62 KB
Version: Version 2.00
(C) 2007 Microsoft Corporation. All rights reserved.
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
123456789.:,;(:*!?')
12 The quick brown fox jumps over the lazy dog. 1234567890
18 The quick brown fox jumps over the lazy dog. 1234567890
24 The quick brown fox jumps over the lazy dog. 1234
36 The quick brown fox jumps over tl
48 The quick brown fox jump
50 The quick brown fox

Font information from Font Viewer

The Big Teacher: Flame

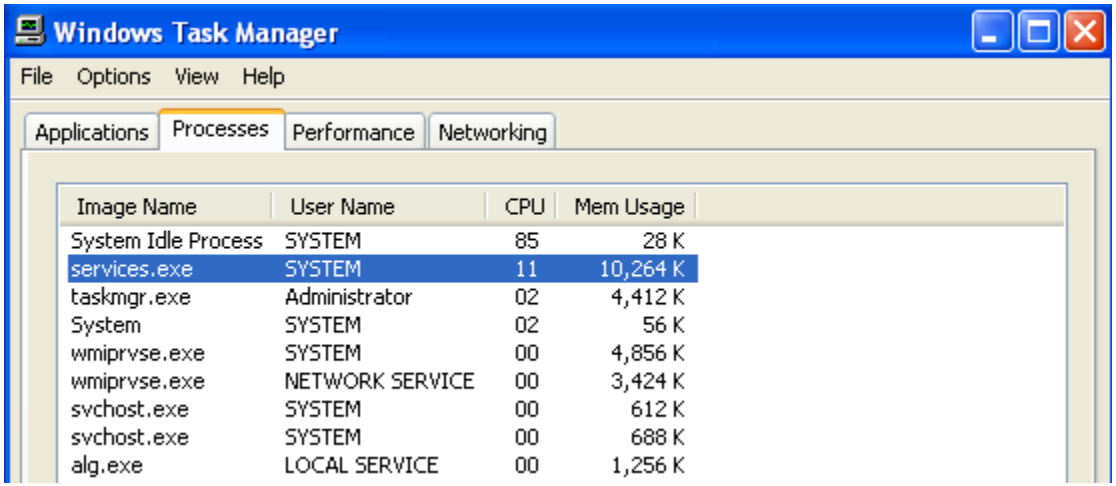
- **The Flame Theory, Detect Flame with 7 simple ways**

1.via Gmer Anti Malware Tool



2. Via Task manager

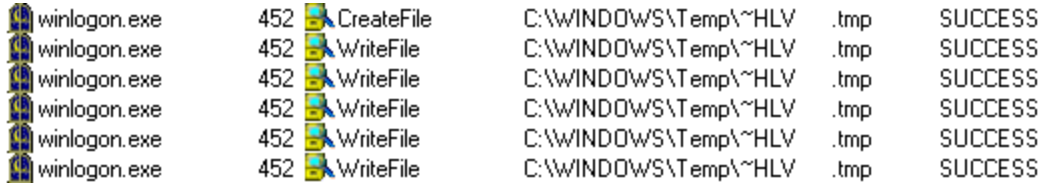
- The infected machine has 10MB Memory Usage for Services.exe and 11% of CPU Usage , but the normal Value is 0~1% CPU Usage and 3MB Memory.


Windows Task Manager
File Options View Help
Applications Processes Performance Networking
Image Name User Name CPU Mem Usage
System Idle Process SYSTEM 85 28 K
services.exe SYSTEM 11 10,264 K
taskmgr.exe Administrator 02 4,412 K
System SYSTEM 02 56 K
wmiprvse.exe SYSTEM 00 4,856 K
wmiprvse.exe NETWORK SERVICE 00 3,424 K
svchost.exe SYSTEM 00 612 K
svchost.exe SYSTEM 00 688 K
alg.exe LOCAL SERVICE 00 1,256 K

csrss.exe	680	SYSTEM	0	00	6,060 K	0 K
winlogon.exe	704	SYSTEM	0	00	6,132 K	0 K
services.exe	748	SYSTEM	0	00	3,944 K	0 K
lsass.exe	760	SYSTEM	0	00	1,320 K	0 K
svchost.exe	920	SYSTEM	0	00	6,048 K	0 K

3. via Process Monitor

- Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.

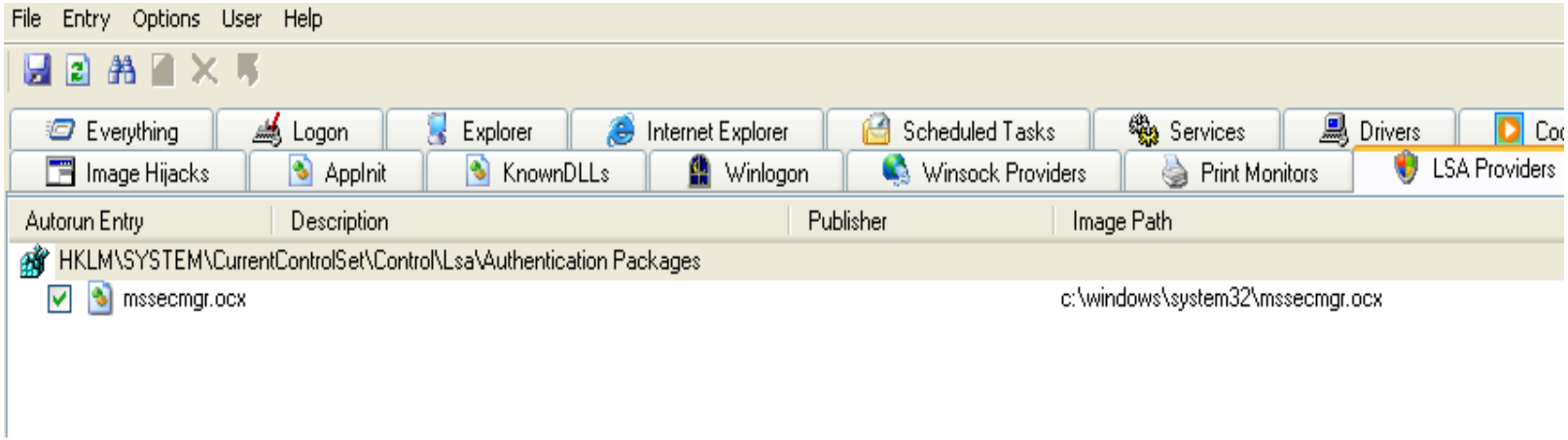


winlogon.exe	452	CreateFile	C:\WINDOWS\Temp\~HLV	.tmp	SUCCESS
winlogon.exe	452	WriteFile	C:\WINDOWS\Temp\~HLV	.tmp	SUCCESS
winlogon.exe	452	WriteFile	C:\WINDOWS\Temp\~HLV	.tmp	SUCCESS
winlogon.exe	452	WriteFile	C:\WINDOWS\Temp\~HLV	.tmp	SUCCESS
winlogon.exe	452	WriteFile	C:\WINDOWS\Temp\~HLV	.tmp	SUCCESS
winlogon.exe	452	WriteFile	C:\WINDOWS\Temp\~HLV	.tmp	SUCCESS

\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS
\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat	services.exe	496 WriteFile	SUCCESS

4. via AutoRuns by Autoruns.exe

- Autoruns.exe, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login.



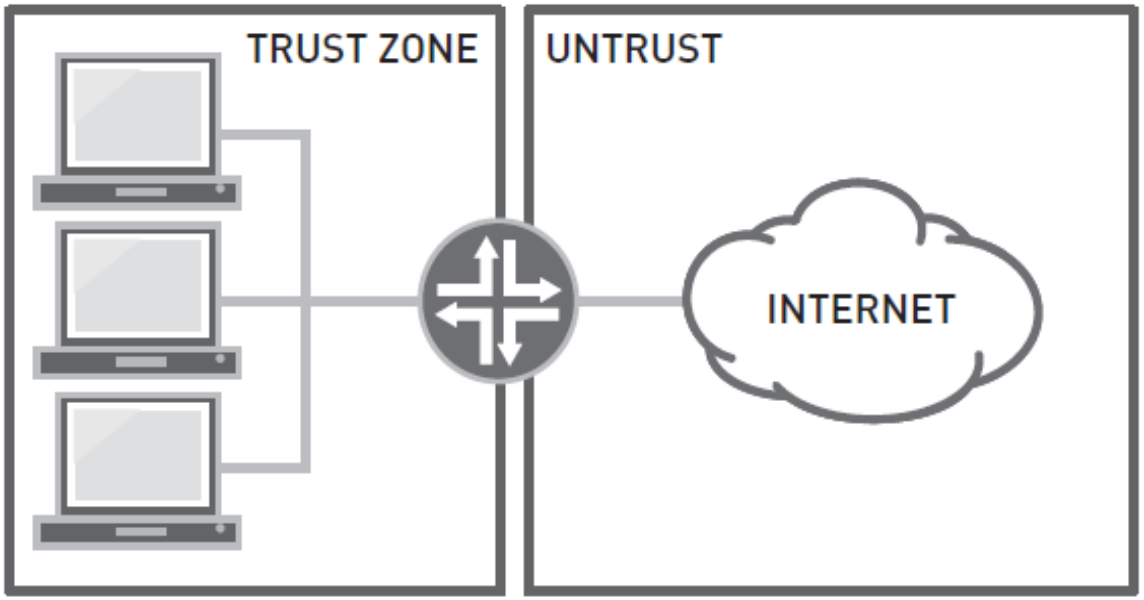
5. via Process Explorer Verification

- Process Explorer is an advanced process management utility that picks up where Task Manager leaves off. It will show you detailed information about a process including its icon, command-line, full image path and memory.

Name	Description	Company Name	Version	Verified Signer
advnetcfg.ocx	Advanced Network ...	Microsoft Corporation	5.1.2600.0	(Unable to verify) Microsoft Corporation
msglu32.ocx	Windows Indexing S...	Microsoft Corporation	5.1.2600.0	(Unable to verify) Microsoft Corporation
mssecmgr.ocx	Windows Authentica...	Microsoft Corporation	5.1.2600.0	(Unable to verify) Microsoft Corporation
nteps32.ocx	Windows NT Enhan...	Microsoft Corporation	5.1.2600.0	(Unable to verify) Microsoft Corporation
COMDLG32.OCX	CMDialog ActiveX C...	Microsoft Corporation	6.0.81.69	(Verified) Microsoft Corporation

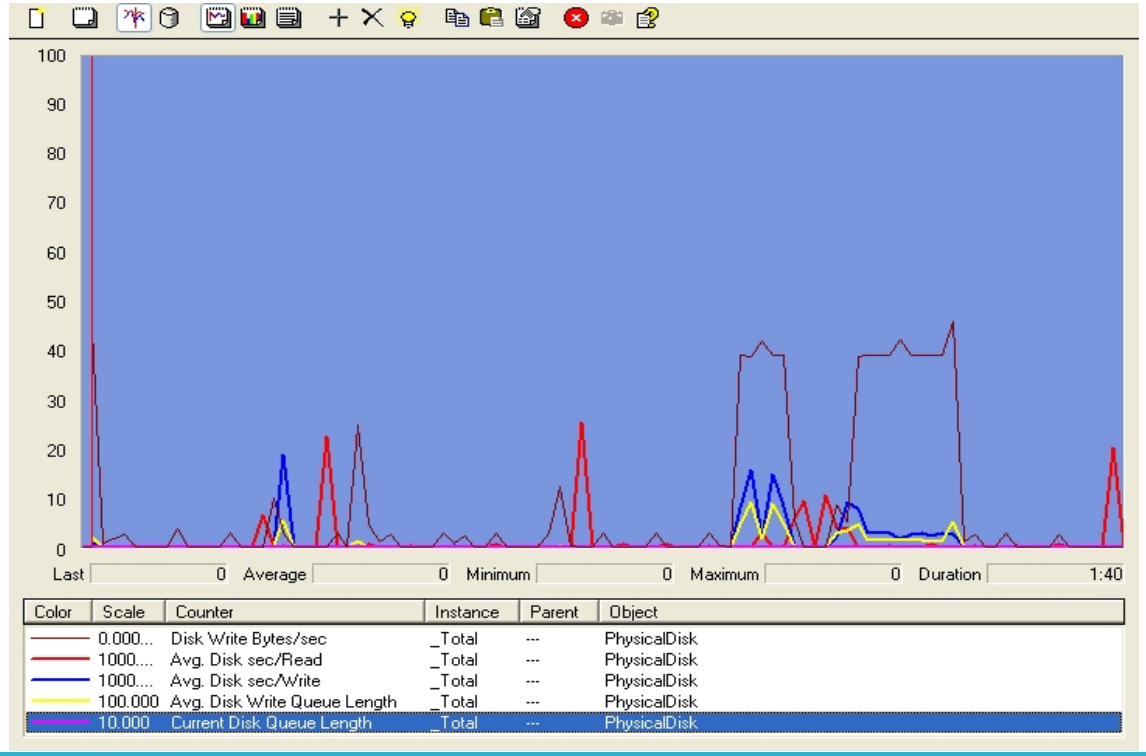
6. Monitoring the TCP/IP Packets

- Flame worm tries to spread Via Network Zero Days; most of time firewalls permit any programs on Domain Controllers to send packets to the Child DCs but with Flame it does not automatically spread, but if you did install some IDS or UTM on your machine you would be capable of identifying the Flame's activity.



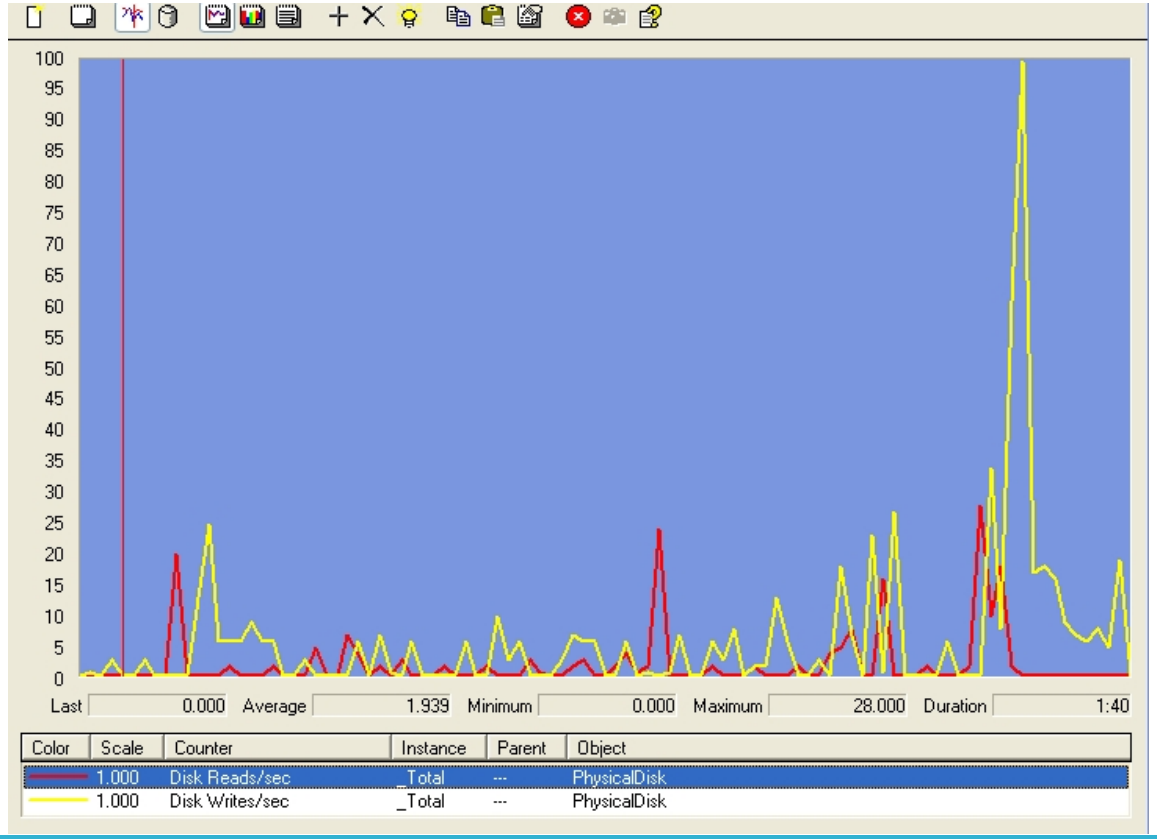
7. Flame's DISK Device I/O

- When Flame will be run under target's machine it has lots of Disk Read and Write. A wise administrator could detect the HDD abnormal Activity and he/she will be able to analyze the infected system.



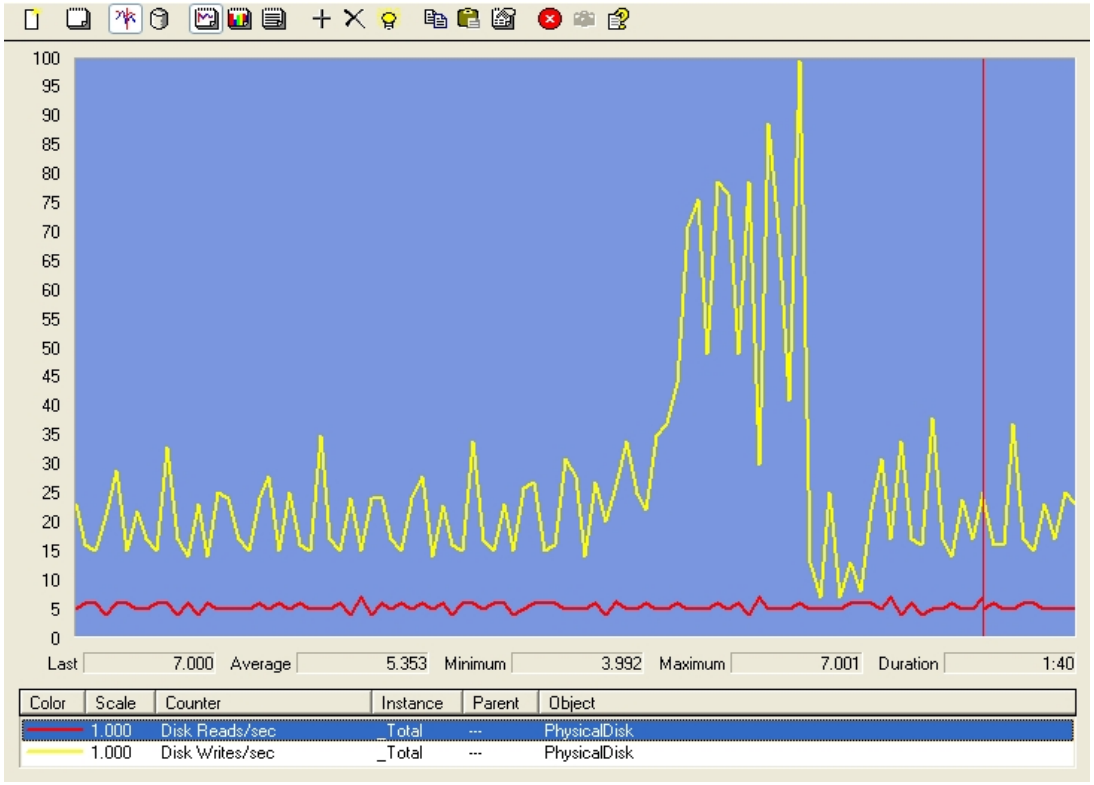
Flame's DISK Device I/O

- Normal Disk Read/Write on Physical HDD



Flame's DISK Device I/O

- A Flame infected system Disk Read/Write on Physical HDD



The Lesson Learned:

- Flame malware bypassed our Anti Malware

Our anti malware could monitor the registry keys

Flame Malware used this key for its own startup

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

The Lesson Learned :

- Our tool was capable of detecting Flame malware but when it tried to raise an alarm , the Flame's data contained some unknown character "null character" and unfortunately the Microsoft component then cut the string.

- msv1_0 + mssecmgr.ocx

- "Authentication Packages"=

hex(7):6d,00,73,00,76,00,31,00,5f,00,30,**00,00,00,6d,**

00,73,00,73,00,65,00,63,00,6d,00,67,00,72,00,2e,00,6f,00,
63,00,78,00,00,00,\00,00

The Most Complex Worm Ever !

- Discovered new virus in February 2012 and contacted Microsoft MMPC and CERT team.

In Memoriam - Tareq Saade

What were the Malware Specifics?

This is the malware features :

1.The worm will blocked any kernel driver installation
(you cannot install any antivirus or anti malware with kernel capability)

2.when you execute any program ,the worm will execute WMP.exe
(we checked the registry key like
"HKEY_CLASSES_ROOT\exefile\shell\Cmd\command" This is not manipulated !)

The worm worked with the other mechanism.

3. there is 2 "Explorer.exe" on the system (one lunched by SVChost.exe and the other is normal)

4.there is no installed kernel driver on it (the system and windows are X64 platform)

All kernel drivers belong to Microsoft and the other vendors are signed.

We ran the system with "Safemode" but the worm work in Safemode too.
(The only way to bypass worm activity is "Safe mode with command prompt)

5.the worm installed a Debugger on the system.
"IsDebuggerPresent" Function Result is true.

6. we try to enumerate processes with "EnumProcessModules" and "OpenProcess"
but the result is nothing. (seems the worm hooked those functions too)

7. we try to install more than 20 antivirus product and kernel land tools but all these tools had failed to install own driver on the infected system.

It seems virus ran another "Explorer.exe" and attached a module on it and try to block access to module list via a kernel driver technique.
we try to use "NtQuerySystemInformation" and "NtQueryObject" to enum Kernel Drivers, but Virus driver hooked these function on the kernel land.

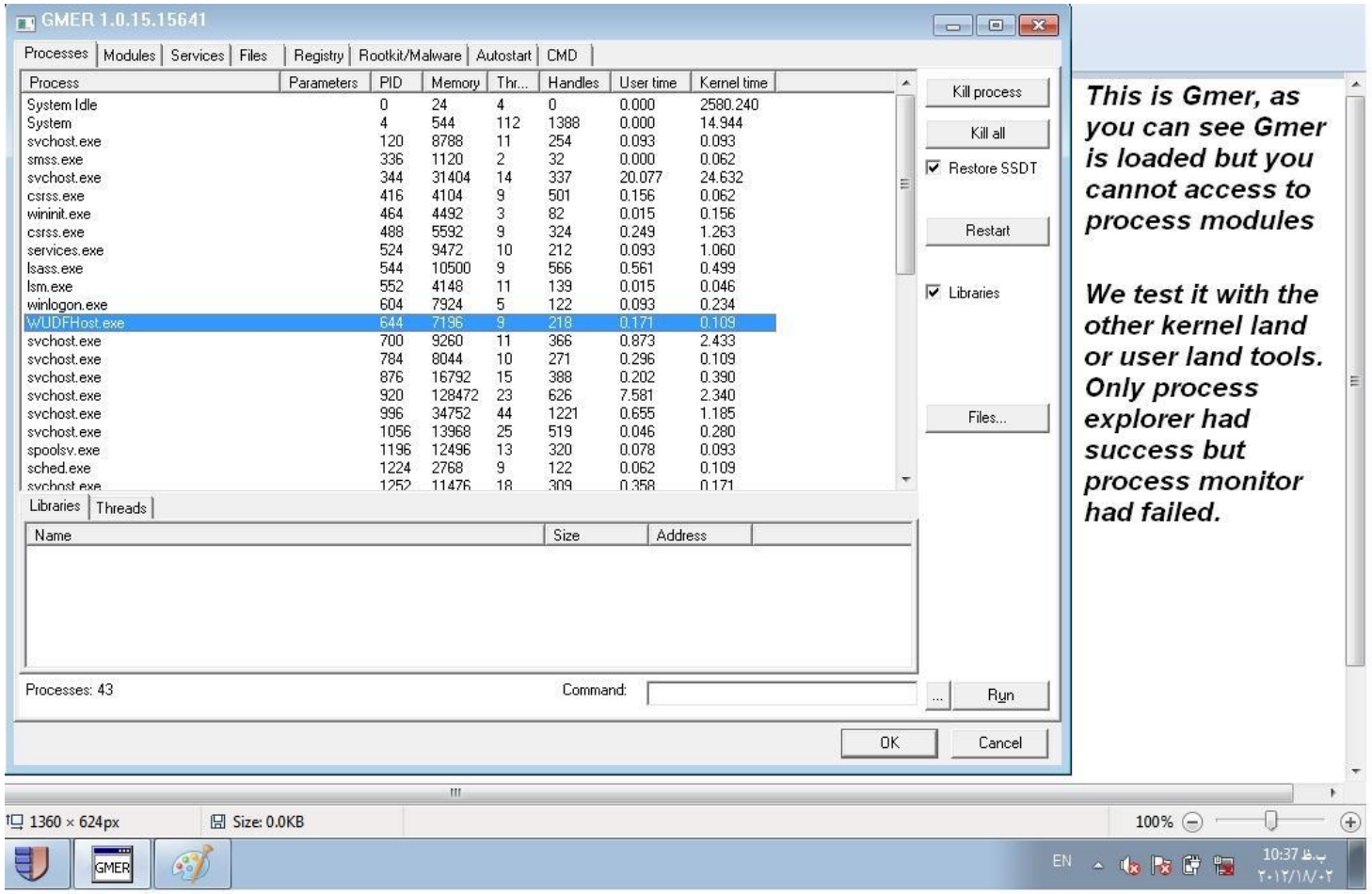
we did not find out anything special and it seems all kernel Drivers are signed.

And the final thing is we cannot install some Monitors Program like "API Monitor" or "Process Monitor"
Both had failed to ran.

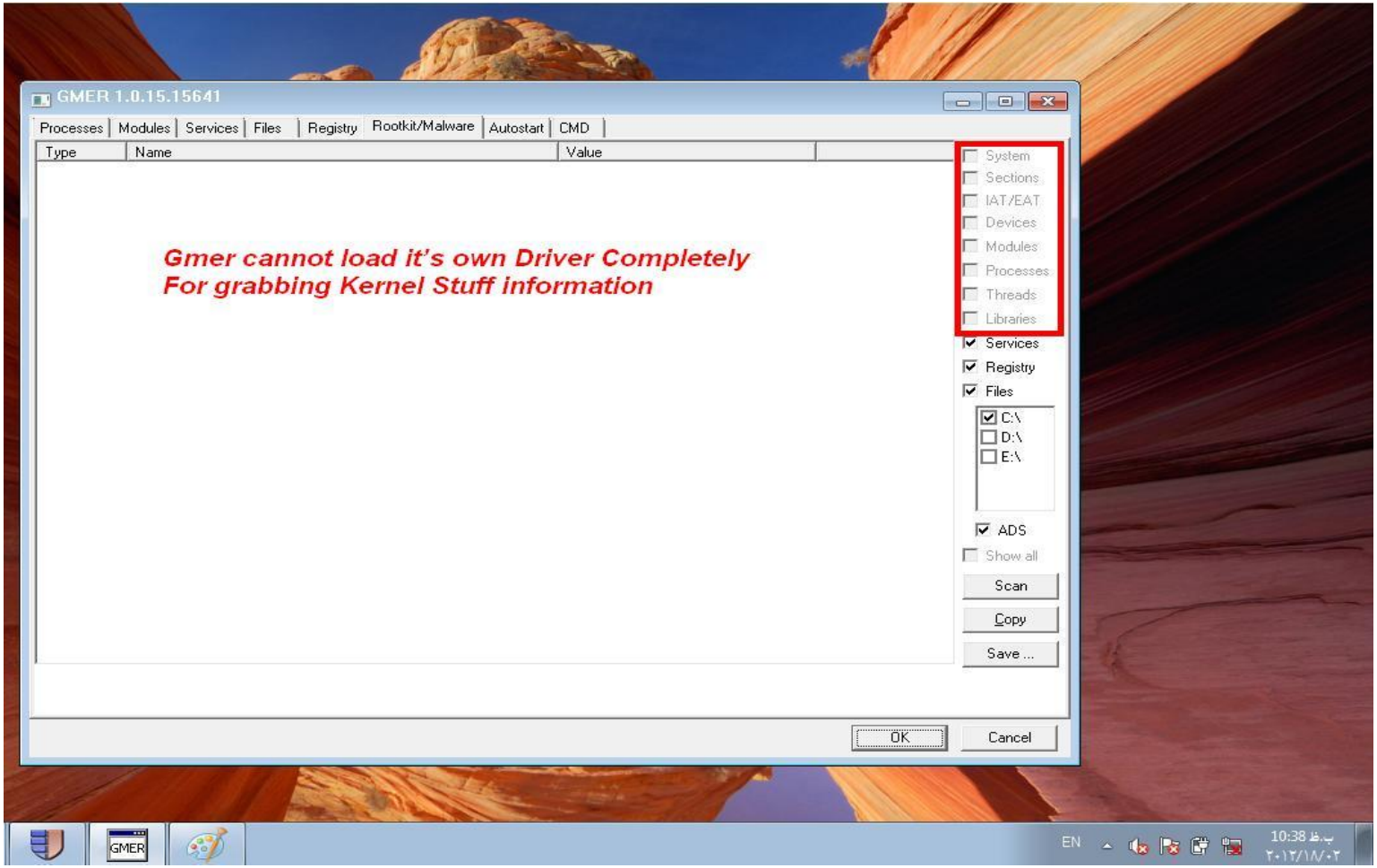
What were the Malware's Capabilities?

- It evaded most Anti Viruses
- It was hidden from most modern Anti Rootkits
- It has some zero days exploits (Signed Kernel Drivers or Stolen Rogue Certificate)
- It prevented you from installing any Kernel Driver to bypass module
- It means when you understood you had virus infection you could not remove it (imagine if this malware was installed on some power plant cycle , you would have to shut down all systems and also reinstall all system operations)

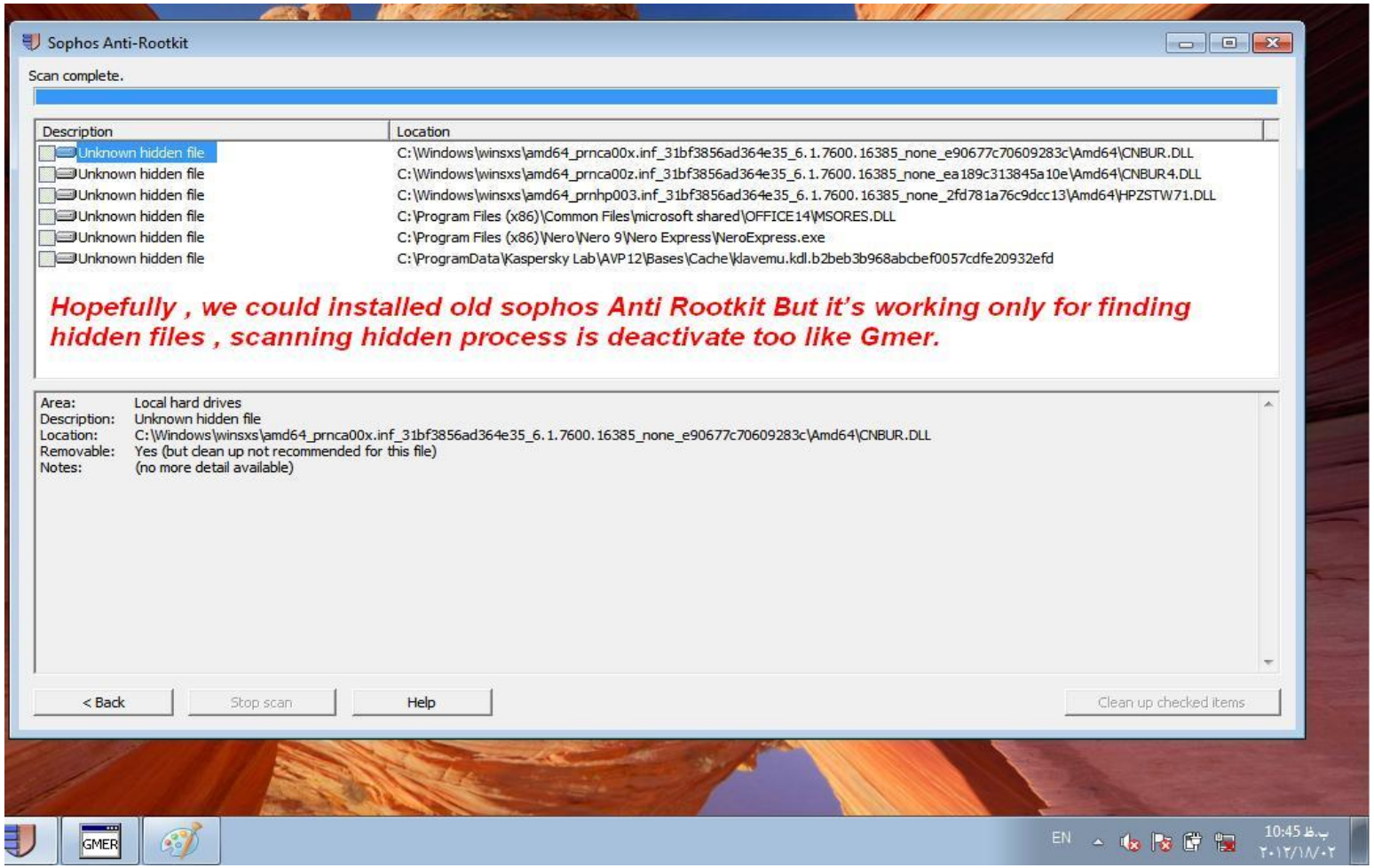
The Malware Pictures



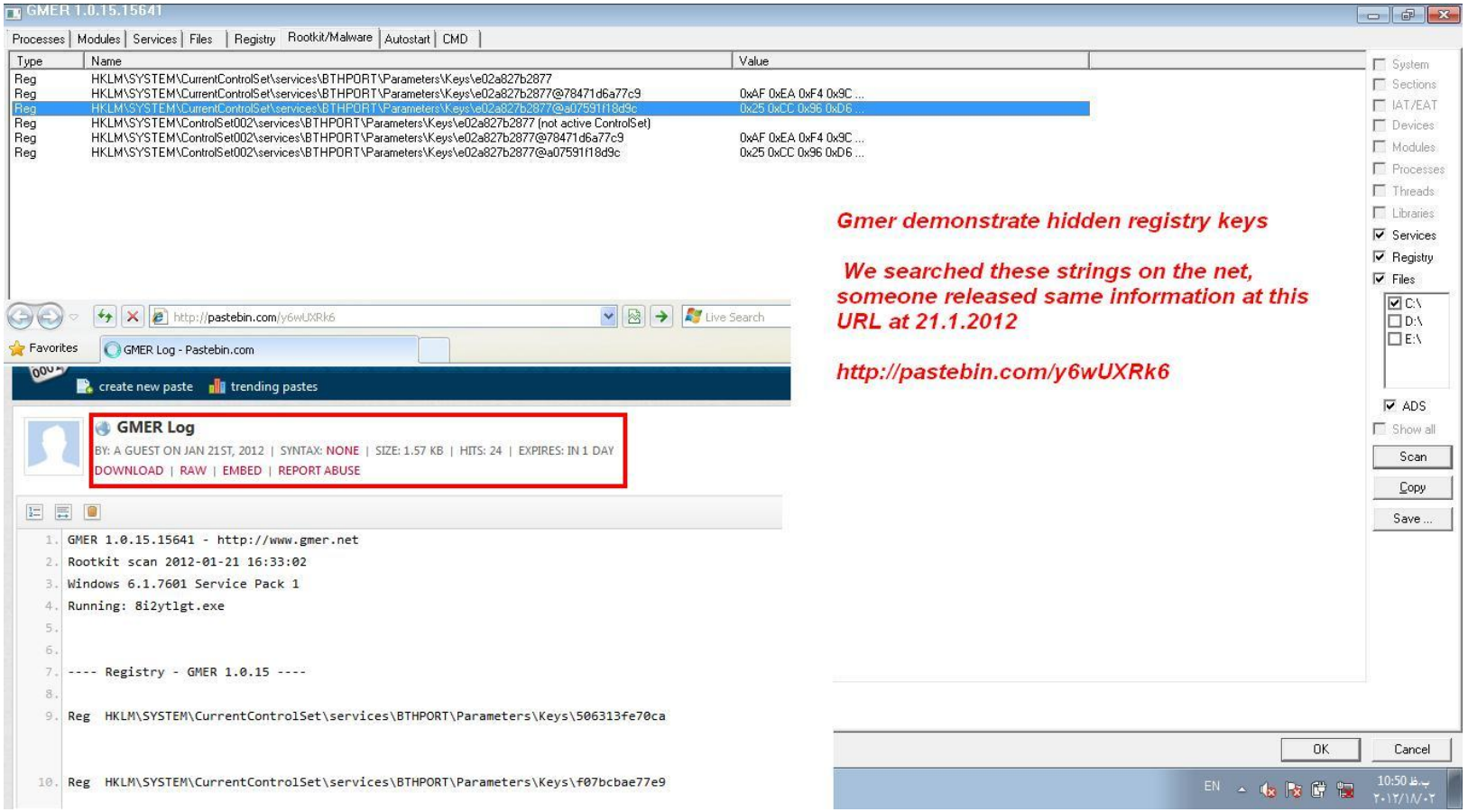
The Malware Pictures



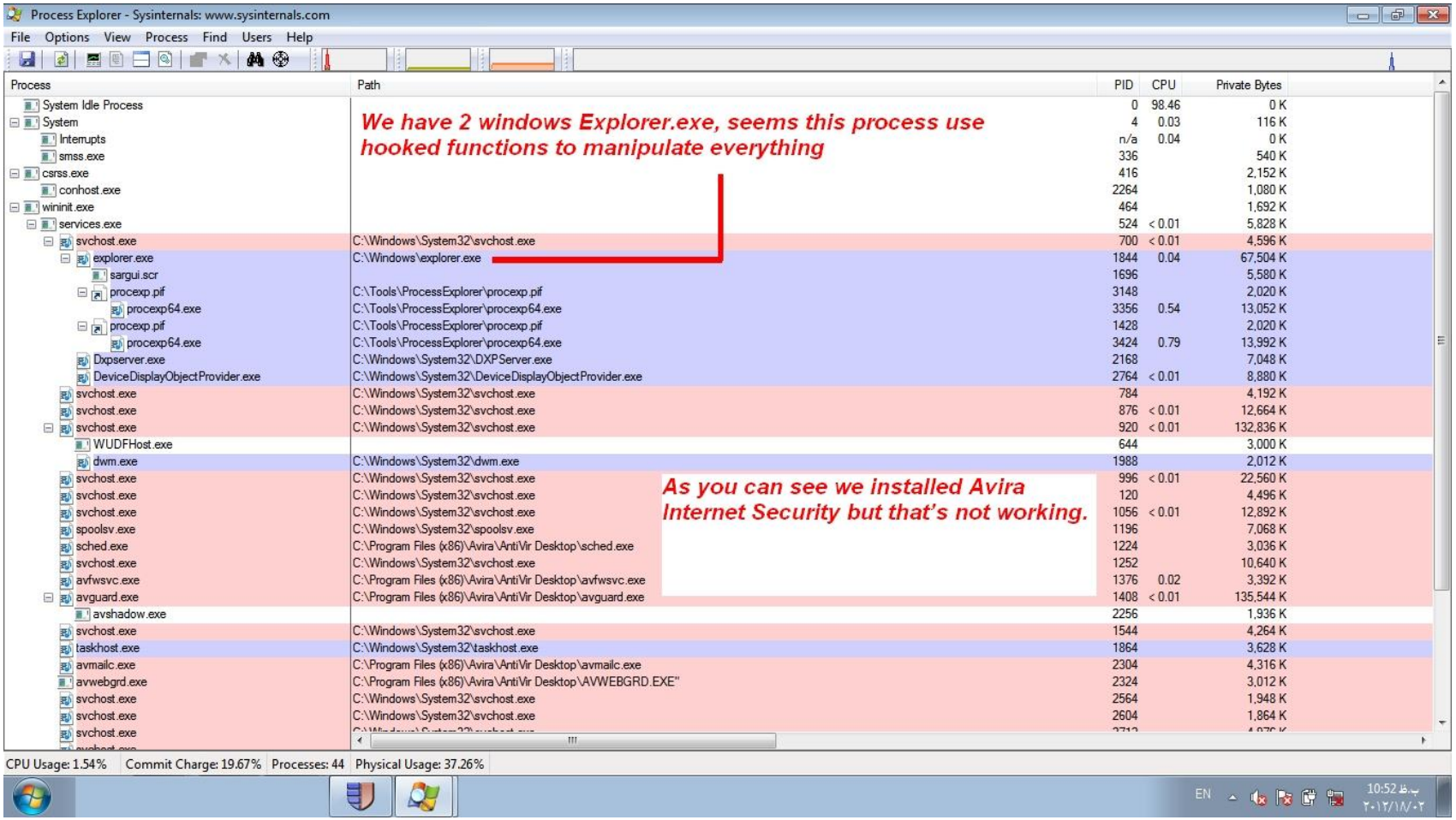
The Malware Pictures



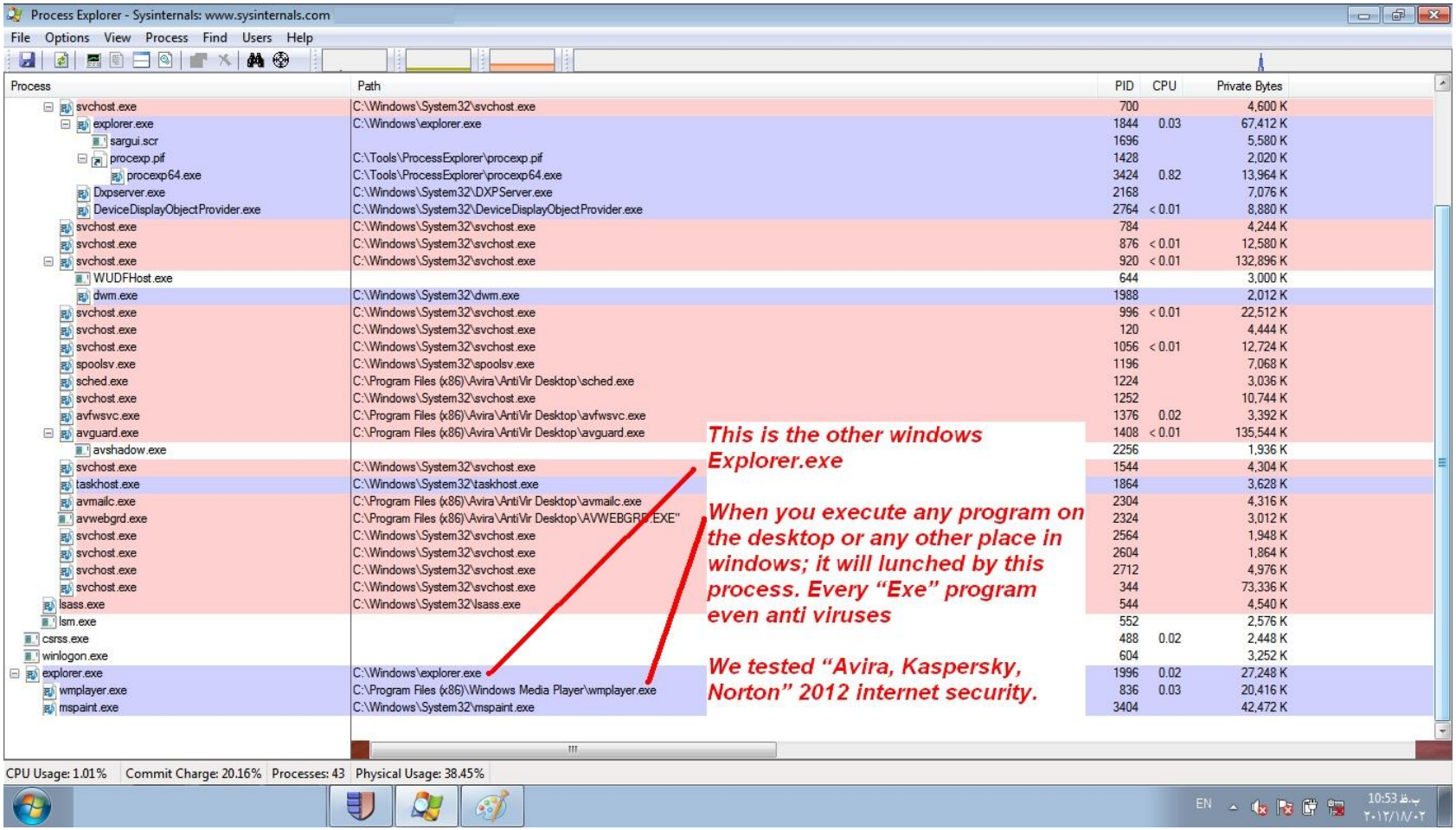
The Malware Pictures



The Malware Pictures


Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Users Help
We have 2 windows Explorer.exe, seems this process use hooked functions to manipulate everything
As you can see we installed Avira Internet Security but that's not working.
CPU Usage: 1.54% Commit Charge: 19.67% Processes: 44 Physical Usage: 37.26%

The Malware Pictures


Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Users Help
Process | Path | PID | CPU | Private Bytes
svchost.exe C:\Windows\System32\svchost.exe 700 4,600 K
explorer.exe C:\Windows\explorer.exe 1844 0.03 67,412 K
sargui.scr 1696 5,580 K
procexp.pif C:\Tools\ProcessExplorer\procexp.pif 1428 2,020 K
procexp64.exe C:\Tools\ProcessExplorer\procexp64.exe 3424 0.82 13,964 K
Dxpserver.exe C:\Windows\System32\DXPServer.exe 2168 7,076 K
DeviceDisplayObjectProvider.exe C:\Windows\System32\DeviceDisplayObjectProvider.exe 2764 < 0.01 8,880 K
svchost.exe C:\Windows\System32\svchost.exe 784 4,244 K
svchost.exe C:\Windows\System32\svchost.exe 876 < 0.01 12,580 K
svchost.exe C:\Windows\System32\svchost.exe 920 < 0.01 132,896 K
WUDFHost.exe 644 3,000 K
dwm.exe C:\Windows\System32\dwm.exe 1988 2,012 K
svchost.exe C:\Windows\System32\svchost.exe 996 < 0.01 22,512 K
svchost.exe C:\Windows\System32\svchost.exe 120 4,444 K
svchost.exe C:\Windows\System32\svchost.exe 1056 < 0.01 12,724 K
spoolsv.exe C:\Windows\System32\spoolsv.exe 1196 7,068 K
sched.exe C:\Program Files (x86)\Avira\AntiVir Desktop\sched.exe 1224 3,036 K
svchost.exe C:\Windows\System32\svchost.exe 1252 10,744 K
avfwsvc.exe C:\Program Files (x86)\Avira\AntiVir Desktop\avfwsvc.exe 1376 0.02 3,392 K
avguard.exe C:\Program Files (x86)\Avira\AntiVir Desktop\avguard.exe 1408 < 0.01 135,544 K
avshadow.exe 2256 1,936 K
svchost.exe C:\Windows\System32\svchost.exe 1544 4,304 K
taskhost.exe C:\Windows\System32\taskhost.exe 1864 3,628 K
avmailc.exe C:\Program Files (x86)\Avira\AntiVir Desktop\avmailc.exe 2304 4,316 K
avwebgrd.exe C:\Program Files (x86)\Avira\AntiVir Desktop\AVWEBGRD.EXE" 2324 3,012 K
svchost.exe C:\Windows\System32\svchost.exe 2564 1,948 K
svchost.exe C:\Windows\System32\svchost.exe 2604 1,864 K
svchost.exe C:\Windows\System32\svchost.exe 2712 4,976 K
svchost.exe C:\Windows\System32\svchost.exe 344 73,336 K
lsass.exe C:\Windows\System32\lsass.exe 544 4,540 K
lsm.exe 552 2,576 K
csrss.exe 488 0.02 2,448 K
winlogon.exe 604 3,252 K
explorer.exe C:\Windows\explorer.exe 1996 0.02 27,248 K
wmplayer.exe C:\Program Files (x86)\Windows Media Player\wmplayer.exe 836 0.03 20,416 K
mspaint.exe C:\Windows\System32\mspaint.exe 3404 42,472 K
This is the other windows Explorer.exe
When you execute any program on the desktop or any other place in windows; it will lunched by this process. Every "Exe" program even anti viruses
We tested "Avira, Kaspersky, Norton" 2012 internet security.
CPU Usage: 1.01% Commit Charge: 20.16% Processes: 43 Physical Usage: 38.45%

Summary

Protect your Network against new malware starting with the following recommendations:

- Use modern and updated Anti Malwares every 2 weeks
- Don’t ever trust your Anti Virus results (Check your system again with other solutions)
- Encrypt all your information and make a backup
- Do not run a Web Server on your network if it is not necessary and block ICMP Packets (Input and Output).
- Use standalone Firewalls (don’t trust Internet security solutions)
- Do not use default settings for your Firewalls or your anti viruses, most default settings are so weak; block applications which are launched by the web browser without user permissions.

The Lessons Learned from Cyber War Malware

www.Nima.tel